University of the Pacific
Scholarly Commons

All Works by Eneström Number
Euler Archive

1738

Observationes de theoremate quodam Fermatiano aliisque ad numeros primos spectantibus

Leonhard Euler

Follow this and additional works at: https://scholarlycommons.pacific.edu/euler-works

Record Created:
2018-09-25

Recommended Citation
Euler, Leonhard, "Observationes de theoremate quodam Fermatiano aliisque ad numeros primos spectantibus" (1738). *All Works by Eneström Number*. 26.
https://scholarlycommons.pacific.edu/euler-works/26

This Article is brought to you for free and open access by the Euler Archive at Scholarly Commons. It has been accepted for inclusion in All Works by Eneström Number by an authorized administrator of Scholarly Commons. For more information, please contact mgibney@pacific.edu.

OBSERVATIONES DE THEOREMATE QVODAM FERMATIANO, ALIISQVE AD NVMEROS PRIMOS SPECTANTIBVS.

AVCTORE
Leonh. Eulero.

Notum eſt hanc quantitatem a^n+1 ſemper habere diuiſores, quoties n ſit numerus impar, vel per imparem praeter vnitatem diuiſibilis. Namque $a^{2m+1}+1$ diuidi poteſt per $a+1$ et $a^{p(2m+1)}+1$ per a^p+1, quicunque etiam numerus loco a ſubſtituatur. Contra vero ſi n fuerit eiusmodi numerus, qui per nullum numerum imparem niſi vnitatem diuidi poſſit, id quod euenit, quando n eſt dignitas binarii, nullus numeri a^n+1 poteſt aſſignari diuiſor. Quamobrem ſi qui ſunt numeri primi huius formae a^n+1, ii omnes comprehendantur neceſſe eſt in hac forma $a^{2^m}+1$. Neque tamen ex hoc poteſt concludi $a^{2^m}+1$ ſemper exhibere numerum primum quicquid ſit a; primo enim perſpicuum eſt, ſi a ſit numerus impar, iſtam formam diuiſorem habiturum 2. Deinde quoque, etiamſi a denotet numerum parem, innumeri tamen dantur caſus, quibus numerus compoſitus prodit. Ita haec ſaltem formula a^2+1 poteſt diuidi per 5, quoties eſt $a=5b\pm 3$, et 30^2+1 poteſt diuidi per 17, et 50^2+1 per 41. Simili modo 10^4+1 habet diuiſorem 73; 6^8+1 habet diuiſorem 17, et $6^{128}+1$ eſt diuiſibilis per 257. At huius formae $2^{2^m}+1$ quan-

quantum ex tabulis numerorum primorum, quae quidem non vltra 100000 extenduntur, nullus detegitur caſus, quo diuiſor aliquis locum habeat. Hac forte aliisque rationibus *Fermatius* adductus enunciare non dubitauit $2^{2^m}+1$ ſemper eſſe numerum primum, hocque vt eximium theorema *Wallifio* aliisque Mathematicis Anglis demonſtrandum propoſuit. Ipſe quidem fatetur ſe eius demonſtrationem non habere, nihilo tamen minus aſſerit eſſe veriſſimum. Vtilitatem eius autem hanc potiſſimum praedicat, quod eius ope facile ſit numerum primum quouis dato maiorem exhibere, id quod ſine huiusmodi vniuerſali theoremate foret difficillimum. Leguntur haec in *Walliſii* Commercio Epiſtolico Tomo Eius Operum ſecundo inſerto, epiſtola penultima. Extant etiam in ipſius *Fermatii* operibus p. 115. ſequentia. "Cum autem numeros a binario quadratice "in ſe ductos et vnitate auctos eſſe ſemper numeros "primos apud me conſtet, et iam dudum Analyſtis il"lius theorematis veritas fuerit ſignificata nempe eſſe "primos 3, 5, 17, 257, 65537, etc. in infinit. nullo "negotio etc.

Veritas iſtius theorematis elucet, vt iam dixi, ſi pro *m* ponatur 1, 2, 3 et 4, prodeunt enim hi numeri 5, 17, 257, et 65537, qui omnes inter numeros primos in tabula reperiuntur. Sed neſcio, quo fato eueniat, vt ſtatim ſequens nempe $2^{2^5}+1$ ceſſet eſſe numerus primus, obſeruaui enim his diebus longe alia agens poſſe hunc numerum diuidi per 641, vt cuique tentanti ſtatim patebit.

Eſt

Eſt enim $2^{2^5}+1 = 2^{32}+1 = 4294967297$. Ex quo intelligi poteſt, theorema hoc etiam in aliis, qui ſequuntur, caſibus fallere, et hanc ob rem problema de inueniendo numero primo quouis dato maiore etiam nunc non eſſe ſolutum.

Conſiderabo nunc etiam formulam 2^n-1, quae quoties n non eſt numerus primus, habet diuiſores: neque tantum 2^n-1 ſed atiam a^n-1. Sed ſi n ſit numerus primus, videri poſſet etiam 2^n-1 ſemper talem exhibere: hoc tamen aſſeuerare nemo eſt auſus quantum ſcio, cum tam facile potuiſſet refelli. Namque $2^{11}-1$ i.e. 2047 diuiſores habet 23 et 89 et $2^{23}-1$ diuidi poteſt per 47. Video autem Cel. *Wolfium* non ſolum hoc in Elem. Matheſeos editione altera non aduertiſſe, vbi numeros perfectos inueſtigat, atque 2047 inter primos numerat; ſed etiam 511 ſeu 2^9-1 pro tali habet, cum tamen ſit diuiſibilis per 2^3-1 i. e. 7. Dat autem $2^{n-1}(2^n-1)$ numerum perfectum, quoties 2^n-1 eſt primus, debet ergo etiam n eſſe numerus primus. Operae igitur pretium fore exiſtimaui eos notare caſus, quibus 2^n-1 non eſt numerus primus, quamuis n ſit talis. Inueni autem hoc ſemper fieri, ſi ſit $n=4m-1$, atque $8m-1$ fuerit numerus primus, tum enim 2^n-1 ſemper poterit diuidi per $8m-1$. Hinc excludendi ſunt caſus ſequentes, 11, 23, 83, 131, 179, 191, 239, etc. qui numeri pro n ſubſtituti reddunt 2^n-1 numerum compoſitum. Neque tamen reliqui numeri primi omnes loco n poſiti ſatisfaciunt, ſed plures inſuper excipiuntur, ſic obſeruaui $2^{37}-1$ diuidi poſſe per 223, $2^{43}-1$ per

431, $2^{29}-1$ per 1103, $2^{73}-1$ per 439, omnes tamen excludere non eſt in poteſtate. Attamen aſſerere audeo praeter hos caſus notatos, omnes numeros primos minores quam 50, et forte quam 100, efficere $2^{n-1}(2^n-1)$ eſſe numerum perfectum, ſequentibus numeris pro n poſitis, 1, 2, 3, 5, 7, 13, 17, 19, 31, 41, 47, vnde 11. proueniunt numeri perfecti. Deduxi has obſeruationes ex Theoremate quodam non ineleganti, cuius quidem demonſtrationem quoque non habeo, verum tamen de eius veritate ſum certiſſimus. Theorema hoc eſt, a^n-b^n, ſemper poteſt diuidi per $n+1$, ſi $n+1$ fuerit numerus primus atque a et b non poſſint per eum diuidi; eo autem difficiliorem puto eius demonſtrationem eſſe, quia non eſt verum niſi $n+1$ ſit numerus primus. Ex hoc ſtatim ſequitur 2^n-1 ſemper diuidi poſſe per $n+1$, ſi fuerit $n+1$ numerus primus, ſeu cum omnis primus ſit impar praeter 2, hicque ob conditiones theorematis, quia eſt $a=2$, non poſſit adhiberi, poterit $2^{2m}-1$ ſemper diuidi per $2m+1$ ſi $2m+1$ ſit numerus primus. Quare etiam vel 2^m+1 vel 2^m-1 diuidi poterit per $2m+1$. Deprehendi autem 2^m+1 poſſe diuidi, ſi fuerit $m=4p+1$ vel $4p+2$, at 2^m-1 habebit diuiſorem $2m+1$, ſi $m=4p$ vel $4p-1$. Haec perſecutus in multa alia incidi theoremata non minus elegantia, quae eo magis aeſtimanda eſſe puto, quod vel demonſtrari prorſus nequeant, vel ex eiusmodi propoſitionibus ſequantur, quae demonſtrari non poſſunt, primaria igitur hic adiungere viſum eſt.

Theo-

Theorema I. Si fuerit n numerus primus, omnis potentia exponentis $n-1$ per n diuiſa vel nihil vel 1 relinquit.

Theorema II. Manente n numero primo, omnis potentia, cuius exponens eſt $n^{m-1}(n-1)$, diuiſa per n^m vel o vel 1 relinquit.

Theorema III. Sint m, n, p, q, etc. numeri primi inaequales, ſitque A minimus communis diuiduus eorum vnitate minutorum, puta ipſorum $m-1$, $n-1$, $p-1$; $q-1$, etc. his poſitis dico omnem potentiam exponentis A vt a^A diuiſam per $mnpq$ etc. vel o vel 1 relinquere, niſi a diuidi poſſit per aliquem horum numerorum, m, n, p, q etc.

Theorema IV. Denotante $2n+1$ numerum primum poterit 3^n+1 diuidi per $2n+1$, ſi ſit vel $n = 6p+2$ vel $n = 6p+3$: at 3^n-1 diuidi poterit per $2n+1$ ſi ſit vel $n =$ vel $6p$ vel $n = 6p-1$.

Theorema V. 3^n+2^n poteſt diuidi per $2n+1$ ſi ſit $n =$ vel $12p+3$, vel $12p+5$, vel $12p+6$, vel $12p+8$. Atque 3^n-2^n poteſt diuidi per $2n+1$, ſi ſit $n =$ vel $12p$ vel $12p+2$, vel $12p+9$, vel $12p+11$.

Theorema VI. Sub iisdem conditionibus quibus 3^n+2^n poterit etiam 6^n+1 diuidi per $2n+1$; atque 6^n-1 ſub iisdem, quibus 3^n-2^n.